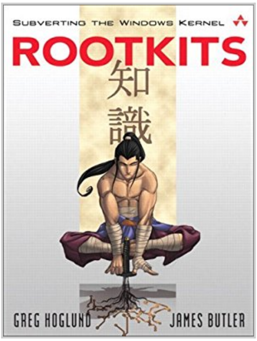

Rootkits: Subverting the Windows Kernel

By Greg Hoglund, Jamie Butler

Rootkits: Subverting the Windows Kernel By Greg Hoglund, Jamie Butler

"It's imperative that everybody working in the field of cyber-security read this book to understand the growing threat of rootkits."
--*Mark Russinovich, editor,* Windows IT Pro / Windows & .NET Magazine
"This material is not only up-to-date, it defines up-to-date. It is truly cutting-edge. As the only book on the subject, ***Rootkits*** will be of interest to any Windows security researcher or security programmer. It's detailed, well researched and the technical information is excellent. The level of technical detail, research, and time invested in developing relevant examples is impressive. In one word: Outstanding."
--*Tony Bautts, Security Consultant; CEO, Xtivix, Inc.*
"This book is an essential read for anyone responsible for Windows security. Security professionals, Windows system administrators, and programmers in general will want to understand the techniques used by rootkit authors. At a time when many IT and security professionals are still worrying about the latest e-mail virus or how to get all of this month's security patches installed, Mr. Hoglund and Mr. Butler open your eyes to some of the most stealthy and significant threats to the Windows operating system. Only by understanding these offensive techniques can you properly defend the networks and systems for which you are responsible."
--*Jennifer Kolde, Security Consultant, Author, and Instructor*
"What's worse than being owned? Not knowing it. Find out what it means to be owned by reading Hoglund and Butler's first-of-a-kind book on rootkits. At the apex the malicious hacker toolset--which includes decompilers, disassemblers, fault-injection engines, kernel debuggers, payload collections, coverage tools, and flow analysis tools--is the rootkit. Beginning where Exploiting Software left off, this book shows how attackers hide in plain sight.

"Rootkits are extremely powerful and are the next wave of attack technology. Like other types of malicious code, rootkits thrive on stealthiness. They hide away from standard system observers, employing hooks, trampolines, and patches to get their work done. Sophisticated rootkits run in such a way that other programs that usually monitor machine behavior can't easily detect them. A rootkit thus provides insider access only to people who know that it is running and available to accept commands. Kernel rootkits can hide files and running processes to provide a backdoor into the target machine.

"Understanding the ultimate attacker's tool provides an important motivator for those of us trying to defend systems. No authors are better suited to give you a detailed hands-on understanding of rootkits than Hoglund and Butler. Better to own this book than to be owned."
--*Gary McGraw, Ph.D., CTO, Cigital, coauthor of* Exploiting Software *(2004) and* Building Secure Software *(2002), both from Addison-Wesley*
"Greg and Jamie are unquestionably the go-to experts when it comes to subverting the Windows API and creating rootkits. These two masters come together to pierce the veil of mystery surrounding rootkits, bringing this information out of the shadows. Anyone even remotely interested in security for Windows systems, including forensic analysis, should include this book very high on their must-read list."
--*Harlan Carvey, author of* Windows Forensics and Incident Recovery *(Addison-Wesley, 2005)*
Rootkits are the ultimate backdoor, giving hackers ongoing and virtually undetectable access to the systems they exploit. Now, two of the world's leading experts have written the first comprehensive guide to rootkits: what they are, how they work, how to build them, and how to detect them. Rootkit.com's Greg Hoglund and James Butler created and teach Black Hat's legendary course in rootkits. In this book, they reveal never-before-told offensive aspects of rootkit technology--learn how attackers can get in and stay in for years, without detection.
Hoglund and Butler show exactly how to subvert the Windows XP and Windows 2000 kernels, teaching concepts that are easily applied to virtually any modern operating system, from Windows Server 2003 to Linux and UNIX. They teach rootkit programming techniques that can be used for a wide range of software, from white hat security tools to operating system drivers and debuggers.
After reading this book, readers will be able to

- Understand the role of rootkits in remote command/control and software eavesdropping
- Build kernel rootkits that can make processes, files, and directories invisible
- Master key rootkit programming techniques, including hooking, runtime patching, and directly manipulating kernel objects
- Work with layered drivers to implement keyboard sniffers and file filters
- Detect rootkits and build host-based intrusion prevention software that resists rootkit attacks

Rootkits: Subverting the Windows Kernel

By Greg Hoglund, Jamie Butler

Rootkits: Subverting the Windows Kernel By Greg Hoglund, Jamie Butler

"It's imperative that everybody working in the field of cyber-security read this book to understand the growing threat of rootkits."
--*Mark Russinovich, editor,* Windows IT Pro / Windows & .NET Magazine
"This material is not only up-to-date, it defines up-to-date. It is truly cutting-edge. As the only book on the subject, ***Rootkits*** will be of interest to any Windows security researcher or security programmer. It's detailed, well researched and the technical information is excellent. The level of technical detail, research, and time invested in developing relevant examples is impressive. In one word: Outstanding."
--*Tony Bautts, Security Consultant; CEO, Xtivix, Inc.*
"This book is an essential read for anyone responsible for Windows security. Security professionals, Windows system administrators, and programmers in general will want to understand the techniques used by rootkit authors. At a time when many IT and security professionals are still worrying about the latest e-mail virus or how to get all of this month's security patches installed, Mr. Hoglund and Mr. Butler open your eyes to some of the most stealthy and significant threats to the Windows operating system. Only by understanding these offensive techniques can you properly defend the networks and systems for which you are responsible."
--*Jennifer Kolde, Security Consultant, Author, and Instructor*
"What's worse than being owned? Not knowing it. Find out what it means to be owned by reading Hoglund and Butler's first-of-a-kind book on rootkits. At the apex the malicious hacker toolset--which includes decompilers, disassemblers, fault-injection engines, kernel debuggers, payload collections, coverage tools, and flow analysis tools--is the rootkit. Beginning where Exploiting Software left off, this book shows how attackers hide in plain sight.

"Rootkits are extremely powerful and are the next wave of attack technology. Like other types of malicious code, rootkits thrive on stealthiness. They hide away from standard system observers, employing hooks, trampolines, and patches to get their work done. Sophisticated rootkits run in such a way that other programs that usually monitor machine behavior can't easily detect them. A rootkit thus provides insider access only to people who know that it is running and available to accept commands. Kernel rootkits can hide files and running processes to provide a backdoor into the target machine.

"Understanding the ultimate attacker's tool provides an important motivator for those of us trying to defend systems. No authors are better suited to give you a detailed hands-on understanding of rootkits than Hoglund and Butler. Better to own this book than to be owned."
--*Gary McGraw, Ph.D., CTO, Cigital, coauthor of* Exploiting Software *(2004) and* Building Secure Software *(2002), both from Addison-Wesley*
"Greg and Jamie are unquestionably the go-to experts when it comes to subverting the Windows API and creating rootkits. These two masters come together to pierce the veil of mystery surrounding rootkits, bringing this information out of the shadows. Anyone even remotely interested in security for Windows systems, including forensic analysis, should include this book very high on their must-read list."
--*Harlan Carvey, author of* Windows Forensics and Incident Recovery *(Addison-Wesley, 2005)*
Rootkits are the ultimate backdoor, giving hackers ongoing and virtually undetectable access to the systems they exploit. Now, two of the world's leading experts have written the first comprehensive guide to rootkits:

what they are, how they work, how to build them, and how to detect them. Rootkit.com's Greg Hoglund and James Butler created and teach Black Hat's legendary course in rootkits. In this book, they reveal never-before-told offensive aspects of rootkit technology--learn how attackers can get in and stay in for years, without detection.
Hoglund and Butler show exactly how to subvert the Windows XP and Windows 2000 kernels, teaching concepts that are easily applied to virtually any modern operating system, from Windows Server 2003 to Linux and UNIX. They teach rootkit programming techniques that can be used for a wide range of software, from white hat security tools to operating system drivers and debuggers.
After reading this book, readers will be able to

- Understand the role of rootkits in remote command/control and software eavesdropping
- Build kernel rootkits that can make processes, files, and directories invisible
- Master key rootkit programming techniques, including hooking, runtime patching, and directly manipulating kernel objects
- Work with layered drivers to implement keyboard sniffers and file filters
- Detect rootkits and build host-based intrusion prevention software that resists rootkit attacks

Rootkits: Subverting the Windows Kernel By Greg Hoglund, Jamie Butler Bibliography

- Sales Rank: #409917 in Books
- Published on: 2005-08-01
- Released on: 2005-07-22
- Original language: English
- Number of items: 1
- Dimensions: 8.90" h x .80" w x 6.90" l, 1.47 pounds
- Binding: Paperback
- 352 pages

Download Rootkits: Subverting the Windows Kernel ...pdf

Read Online Rootkits: Subverting the Windows Kernel ...pdf

Download and Read Free Online Rootkits: Subverting the Windows Kernel By Greg Hoglund, Jamie Butler

Editorial Review

From the Back Cover

"It's imperative that everybody working in the field of cyber-security read this book to understand the growing threat of rootkits."
"--Mark Russinovich, editor, " Windows IT Pro / Windows & .NET Magazine

"This material is not only up-to-date, it defines up-to-date. It is truly cutting-edge. As the only book on the subject, "Rootkits" will be of interest to any Windows security researcher or security programmer. It's detailed, well researched and the technical information is excellent. The level of technical detail, research, and time invested in developing relevant examples is impressive. In one word: Outstanding."
"--Tony Bautts, Security Consultant; CEO, Xtivix, Inc."

"This book is an essential read for anyone responsible for Windows security. Security professionals, Windows system administrators, and programmers in general will want to understand the techniques used by rootkit authors. At a time when many IT and security professionals are still worrying about the latest e-mail virus or how to get all of this month's security patches installed, Mr. Hoglund and Mr. Butler open your eyes to some of the most stealthy and significant threats to the Windows operating system. Only by understanding these offensive techniques can you properly defend the networks and systems for which you are responsible."
"--Jennifer Kolde, Security Consultant, Author, and Instructor"

"What's worse than being owned? Not knowing it. Find out what it means to be owned by reading Hoglund and Butler's first-of-a-kind book on rootkits. At the apex the malicious hacker toolset--which includes decompilers, disassemblers, fault-injection engines, kernel debuggers, payload collections, coverage tools, and flow analysis tools--is the rootkit. Beginning where Exploiting Software left off, this book shows how attackers hide in plain sight.
"Rootkits are extremely powerful and are the next wave of attack technology. Like other types of malicious code, rootkits thrive on stealthiness. They hide away from standard system observers, employing hooks, trampolines, and patches to get their work done. Sophisticated rootkits run in such a way that other programs that usually monitor machine behavior can't easily detect them. A rootkit thus provides insider access only to people who know that it is running and available to accept commands. Kernel rootkits can hide files and running processes to provide a backdoor into the target machine.
"Understanding the ultimate attacker's tool provides an important motivator for those of us trying to defend systems. No authors are better suited to give you a detailed hands-on understanding of rootkits than Hoglund and Butler. Better to own this book than to be owned."
"--Gary McGraw, Ph.D., CTO, Cigital, coauthor of" Exploiting Software "(2004) and" Building Secure Software "(2002), both from Addison-Wesley"

"Greg and Jamie are unquestionably the go-to experts when it comes to subverting the Windows API and creating rootkits. These two masters come together to pierce the veil of mystery surrounding rootkits, bringing this information out of the shadows. Anyone even remotely interested in security for Windows systems, including forensic analysis, should include this book very high on their must-read list."
"--Harlan Carvey, author of" Windows Forensics and Incident Recovery "(Addison-Wesley, 2005)"

Rootkits are the ultimate backdoor, giving hackers ongoing and virtually undetectable access to the systems they exploit. Now, two of the world's leading experts have written the first comprehensive guide to rootkits: what they are, how they work, how to build them, and how to detect them. Rootkit.com's Greg Hoglund and James Butler created and teach Black Hat's legendary course in rootkits. In this book, they reveal never-before-told offensive aspects of rootkit technology--learn how attackers can get in and stay in for years, without detection.

Hoglund and Butler show exactly how to subvert the Windows XP and Windows 2000 kernels, teaching concepts that are easily applied to virtually any modern operating system, from Windows Server 2003 to Linux and UNIX. Using extensive downloadable examples, they teach rootkit programming techniques that can be used for a wide range of software, from white hat security tools to operating system drivers and debuggers.

After reading this book, readers will be able toUnderstand the role of rootkits in remote command/control and software eavesdroppingBuild kernel rootkits that can make processes, files, and directories invisibleMaster key rootkit programming techniques, including hooking, runtime patching, and directly manipulating kernel objectsWork with layered drivers to implement keyboard sniffers and file filtersDetect rootkits and build host-based intrusion prevention software that resists rootkit attacks

Visit rootkit.com for code and programs from this book. The site also contains enhancements to the book's text, such as up-to-the-minute information on rootkits available nowhere else.

About the Author

Greg Hoglund has been a pioneer in the area of software security. He is CEO of HBGary, Inc., a leading provider of software security verification services. After writing one of the first network vulnerability scanners (installed in over half of all Fortune 500 companies), he created and documented the first Windows NT-based rootkit, founding rootkit.com in the process. Greg is a frequent speaker at Black Hat, RSA, and other security conferences.

James Butler, Director of Engineering at HBGary, has a world-class talent for kernel programming and rootkit development and extensive experience in host-based intrusion-detection systems. He is the developer of VICE, a rootkit detection and forensics system. Jamie's previous positions include Senior Security Software Engineer at Enterasys and Computer Scientist at the National Security Agency. He is a frequent trainer and speaker at Black Hat security conferences. He holds a masters of computer science from the University of Maryland, Baltimore County. He has published articles in the *IEEE Information Assurance Workshop,* Phrack, USENIX ;login:, and *Information Management* and *Computer Security.*

Excerpt. © Reprinted by permission. All rights reserved.

A rootkit is a set of programs and code that allows a permanent and undetectable presence on a computer.

Historical Background

We became interested in rootkits because of our professional work in computer security, but the pursuit of the subject quickly expanded into a personal mission (also known as late nights and weekends). This led Hoglund to found rootkit.com, a forum devoted to reverse engineering and rootkit development. Both of us are deeply involved with rootkit.com. Butler first contacted Hoglund online through this Web site because Butler had a new and powerful rootkit called FU that needed testing, [1] Butler sent Hoglund some source code and a pre-compiled binary. However, by accident, he did not send Hoglund the source code to the kernel driver. To Butler's amazement, Hoglund just loaded the pre-compiled rootkit onto his workstation without question, and reported back that FU seemed to be working fine! Our trust in one another has only grown since then. [2]

Both of us have long been driven by an almost perverse need to reverse-engineer the Windows kernel. It's like when someone says we can't do something--then we accomplish it. It is very satisfying learning how so-called computer security products work and finding ways around them. This inevitably leads to better protection mechanisms.

The fact that a product claims to provide some level of protection does not necessarily mean it actually does. By playing the part of an attacker, we are always at an advantage. As the attacker we must think of only one thing that a defender didn't consider. Defenders, on the other hand, must think of every possible thing an attacker might do. The numbers work in the attacker's favor.

We teamed up a few years ago to offer the training class "Offensive Aspects of Rootkit Technology." This training started as a single day of material that since has grown to include hundreds of pages of notes and example code. The material for the class eventually became the foundation for this book. We now offer the rootkit training class several times a year at the Black Hat security conference, and also privately.

After training for awhile, we decided to deepen our relationship, and we now work together at HBGary, Inc. At HBGary, we tackle very complex rootkit problems on a daily basis. In this book, we use our experience to cover the threats that face Windows users today, and likely will only increase in the future.

Target Audience

This book is intended for those who are interested in computer security and want a truer perspective concerning security threats. A lot has been written on how intruders gain access to computer systems, but little has been said regarding what can happen once an intruder gains that initial access. Like the title implies, this book will cover what an intruder can do to cover her presence on a compromised machine.

We believe that most software vendors, including Microsoft, do not take rootkits seriously. That is why we are publishing this book. The material in this book is not groundbreaking for someone who has worked with rootkits or operating systems for years--but for most people this book should prove that rootkits are a serious threat. It should prove that your virus scanner or desktop firewall is never good enough. It should prove that a rootkit can get into your computer and stay there for years without you ever knowing about it.

To best convey rootkit information, we wrote most of this book from an attacker's perspective; however, we end the book on a defensive posture. As you begin to learn your attackers' goals and techniques, you will begin to learn your own system's weaknesses and how to mitigate its shortcomings. Reading this book will help you improve the security of your system or help you make informed decisions when it comes to purchasing security software.

Prerequisites

As all of the code samples are written in C, you will gain more insight if you already understand basic C concepts--the most important one being pointers. If you have no programming knowledge, you should still be able to follow along and understand the threats without needing to understand the particular implementation details. Some areas of the book draw on principles from the Windows device driver architecture, but experience writing device drivers is not required. We will walk you through writing your first Windows device driver and build from there.

Scope

This book covers Windows rootkits, although most of the concepts apply to other operating systems as well, such as LINUX. We focus on kernel rootkits because these are the most difficult to detect. Many public rootkits for Windows are userland rootkits [3] because these are the easiest to implement, since they do not involve the added complexity of understanding how the undocumented kernel works.

This book is not about specific real-world rootkits. Rather, it teaches the generic approaches used by all rootkits. In each chapter, we introduce a basic technique, explain its purposes, and show how it's implemented using code examples. Armed with this information, you should be able to expand the examples in a million different ways to perform a variety of tasks. When working in the kernel, you are really limited only by your imagination.

You can download most of the code in this book from rootkit.com. Throughout the book, we will reference the particular URL for each individual example. Other rootkit authors also publish research at rootkit.com that you may find useful for keeping up with the latest discoveries.

1. Butler was not interested in rootkits for malicious purposes. He was instead fascinated with the power of kernel modifications. This led Butler to develop one of the first rootkit-detection programs, VICE.

2. Hoglund still wonders, from time to time, whether that original version of FU is still running on his workstation.

3. Userland rootkits are rootkits that do not employ kernel-level modifications, but instead rely only upon user-program modifications.

0321294319P07072005

Users Review

From reader reviews:

Ila Robinette:

Do you among people who can't read pleasant if the sentence chained in the straightway, hold on guys this particular aren't like that. This Rootkits: Subverting the Windows Kernel book is readable by simply you who hate the straight word style. You will find the info here are arrange for enjoyable reading through experience without leaving also decrease the knowledge that want to offer to you. The writer connected with Rootkits: Subverting the Windows Kernel content conveys thinking easily to understand by most people. The printed and e-book are not different in the content but it just different such as it. So , do you nevertheless thinking Rootkits: Subverting the Windows Kernel is not loveable to be your top collection reading book?

Sadie McBride:

Spent a free time to be fun activity to perform! A lot of people spent their free time with their family, or their own friends. Usually they undertaking activity like watching television, gonna beach, or picnic in the park. They actually doing same every week. Do you feel it? Would you like to something different to fill your own personal free time/ holiday? May be reading a book is usually option to fill your no cost time/ holiday. The first thing that you'll ask may be what kinds of book that you should read. If you want to consider look for book, may be the publication untitled Rootkits: Subverting the Windows Kernel can be very good book to read. May be it may be best activity to you.

Rudy Lapan:

As a college student exactly feel bored for you to reading. If their teacher inquired them to go to the library in order to make summary for some reserve, they are complained. Just very little students that has reading's soul or real their passion. They just do what the teacher want, like asked to go to the library. They go to presently there but nothing reading very seriously. Any students feel that reading through is not important, boring in addition to can't see colorful pictures on there. Yeah, it is being complicated. Book is very important for you personally. As we know that on this age, many ways to get whatever you want. Likewise word says, ways to reach Chinese's country. Therefore , this Rootkits: Subverting the Windows Kernel can make you experience more interested to read.

Herbert Gist:

What is your hobby? Have you heard this question when you got pupils? We believe that that query was given by teacher to their students. Many kinds of hobby, Everybody has different hobby. And also you know that little person such as reading or as reading through become their hobby. You must know that reading is very important as well as book as to be the matter. Book is important thing to add you knowledge, except your current teacher or lecturer. You get good news or update with regards to something by book. Different categories of books that can you choose to use be your object. One of them are these claims Rootkits: Subverting the Windows Kernel.

Download and Read Online Rootkits: Subverting the Windows Kernel By Greg Hoglund, Jamie Butler #4GXQ8ITJ3L7

Read Rootkits: Subverting the Windows Kernel By Greg Hoglund, Jamie Butler for online ebook

Rootkits: Subverting the Windows Kernel By Greg Hoglund, Jamie Butler Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Rootkits: Subverting the Windows Kernel By Greg Hoglund, Jamie Butler books to read online.

Online Rootkits: Subverting the Windows Kernel By Greg Hoglund, Jamie Butler ebook PDF download

Rootkits: Subverting the Windows Kernel By Greg Hoglund, Jamie Butler Doc

Rootkits: Subverting the Windows Kernel By Greg Hoglund, Jamie Butler Mobipocket

Rootkits: Subverting the Windows Kernel By Greg Hoglund, Jamie Butler EPub

4GXQ8ITJ3L7: Rootkits: Subverting the Windows Kernel By Greg Hoglund, Jamie Butler